

HANDREIKING INFORMATIEVEILIGHEID 3D

Concept

Colofon

Naam document

Handreiking informatieveiligheid 3D

Versienummer

concept

Versiedatum

April 2014

Versiebeheer

Het beheer van dit document berust bij de Informatiebeveiligingsdienst voor gemeenten (IBD).

Copyright

© 2014 Kwaliteitsinstituut Nederlandse Gemeenten (KING).

Alle rechten voorbehouden. Verveelvoudiging, verspreiding en gebruik van deze uitgave voor het doel zoals vermeld in deze uitgave is met bronvermelding toegestaan voor alle gemeenten en overheidsorganisaties.

Voor commerciële organisaties wordt hierbij toestemming verleend om dit document te bekijken, af te drukken, te verspreiden en te gebruiken onder de hiernavolgende voorwaarden:

1. KING wordt als bron vermeld;
2. het document en de inhoud mogen commercieel niet geëxploiteerd worden;
3. publicaties of informatie waarvan de intellectuele eigendomsrechten niet bij de verstrekker berusten, blijven onderworpen aan de beperkingen opgelegd door KING;
4. ieder kopie van dit document, of een gedeelte daarvan, dient te zijn voorzien van de in deze paragraaf vermelde mededeling.

Rechten en vrijwaring

KING is zich bewust van haar verantwoordelijkheid een zo betrouwbaar mogelijke uitgave te verzorgen. Niettemin kan KING geen aansprakelijkheid aanvaarden voor eventueel in deze uitgave voorkomende onjuistheden, onvolledigheden of nalatigheden. KING aanvaardt ook geen aansprakelijkheid voor enig gebruik van voorliggende uitgave of schade ontstaan door de inhoud van de uitgave of door de toepassing ervan.

Leeswijzer

Dit product maakt onderdeel uit van het programma VISD (informatievoorziening Sociale Domein) en helpt gemeenten om hun informatiehuishouding op tijd en veilig aan te passen aan de nieuwe taken.

Doel

Het doel van dit document (informatiebeveiliging sociale domein) is het leveren van een overzicht van beveiligingsproducten die gemeenten helpen de juiste aandacht te geven aan de gewenste beveiligingseisen die noodzakelijk zijn. Deze beveiligingseisen zijn afhankelijk van onderkende risico's welke inwerken op de processen, systemen en informatie en dienen te passen binnen de geaccepteerde Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG). Het helpt gemeenten bij het borgen van goede, zorgvuldige en veilige gegevensuitwisseling en procesuitvoering.

Doelgroep

Dit document is van belang voor onder andere de informatiebeveiligingsfunctionarissen / Chief Information Security Officers (CISO) van gemeenten, de verantwoordelijke voor het inrichten van de nieuwe taken naar aanleiding van de decentralisaties binnen de gemeenten en de betrokken architecten, proces- en systeemeigenaren bij de decentralisaties.

Inhoud

1	Inleiding	7
1.1	Informatiebeveiligingsdienst	7
1.2	Informatiebeveiliging en de decentralisaties	7
1.3	Hoe te lezen	8
2	Programma van eisen	10
2.1	inleiding	10
2.2	Archetype	10
2.3	Thema's	10
2.4	Belang thema informatieveiligheid	11
2.5	Uitwisseling (persoons)gegevens binnen het sociale domein	11
3	Informatieveiligheid	14
3.1	Wat is informatieveiligheid?	14
3.2	Veiligheid, privacy en beveiliging in het kader van 3D	14
4	Organisaties in het kader van informatieveiligheid	16
4.1	Informatiebeveiligingsdienst voor gemeenten	16
4.2	Nationaal Cyber Security Centrum (NCSC)	19
4.3	Taskforce Bestuur en Informatieveiligheid Dienstverlening	20
4.4	Centrum voor Informatiebeveiliging en Privacybescherming	21
4.5	College bescherming persoonsgegevens	22
4.6	Overige organisaties	23
5	Aan de slag	25
5.1	Informatiebeveiligingsonderwerpen	25
5.2	Ondersteunde documenten	25

1 Inleiding

Gemeenten zijn voor steeds meer beleidsterreinen verantwoordelijk. Zij maken daarbij gebruik van de mogelijkheden van informatie-uitwisseling. Door informatie te delen en processen te optimaliseren kunnen gemeenten onder andere hun dienstverlening beter organiseren, de veiligheid van burgers verbeteren en meer mensen aan het werk krijgen. Ook voor de drie decentralisatie van taken op gebied van jeugd, zorg en werk zullen gemeenten onderling en met diverse ketenpartners informatie uitwisselen.

Als professionele organisatie past hierbij dat gemeenten ook de beveiliging van informatie professioneel organiseren. Informatie moet immers beschikbaar en betrouwbaar zijn en mag alleen door bevoegden zijn in te zien. Bij de uitwisseling moeten gemeenten voldoende rekening houden met beveiligings- en privacyaspecten.

1.1 Informatiebeveiligingsdienst

De Informatiebeveiligingsdienst voor gemeenten (IBD)¹ is een gezamenlijk initiatief van de Vereniging van Nederlandse Gemeenten (VNG) en het Kwaliteitsinstituut Nederlandse Gemeenten (KING) en actief sinds 1 januari 2013. De IBD is er voor alle gemeenten en richt zich op bewustwording en concrete ondersteuning om gemeenten te helpen hun informatiebeveiliging naar een hoger plan te tillen. De IBD heeft drie concrete doelen. Allereerst het preventief en structureel ondersteunen van gemeenten bij het opbouwen en onderhouden van bewustzijn als het gaat om informatiebeveiliging. In de tweede plaats het leveren van integrale coördinatie en concrete ondersteuning op gemeente specifieke aspecten in geval van incidenten en crisissituaties op het vlak van informatiebeveiliging. En tot slot, gerichte projectmatige ondersteuning op deelgebieden om informatiebeveiliging in de praktijk van alle dag naar een hoger plan te tillen.

De IBD heeft een beperkte scope en verantwoordelijkheid. De gemeenten blijven zelf verantwoordelijk voor hun informatiebeveiliging. Zowel beleidstechnisch als uitvoerend (Propositie Informatiebeveiligingsdienst 2012²).

1.2 Informatiebeveiliging en de decentralisaties

Tijdens de Buitengewone Algemene Ledenvergadering (BALV) van 29 november 2013 hebben de gemeenten de Resolutie 'Informatieveiligheid, randvoorwaarde voor de professionele gemeente' aangenomen. Dit betekent dat iedere gemeente onderschrijft informatieveiligheidsbeleid vast te stellen aan de hand van de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG), die door de IBD is ontwikkeld. Verder stelt de Resolutie dat gemeenten informatieveiligheid zowel bestuurlijk als ambtelijk borgen en transparant maken voor burgers, bedrijven en ketenpartners. De drie decentralisaties voor jeugd, zorg en werk zijn niet als uitgangspunt genomen bij het opstellen van de BIG waardoor het waarschijnlijk nodig is om voor de drie decentralisaties additionele specifieke maatregelen te treffen. Binnen de drie gedecentraliseerde domeinen wordt (zeer) privacygevoelige informatie van burgers verzameld, verwerkt en uitgewisseld. Er is gemeenten en partners veel aangelegen om deze informatie goed te beveiligen.

¹ <http://new.kinggemeenten.nl/informatiebeveiliging>

² <https://new.kinggemeenten.nl/informatiebeveiliging/nieuws/ibd-financiering-informatiebeveiligingsdienst-via-gemeentefonds#>

Het doel is een veilige gegevensuitwisseling binnen de drie gedecentraliseerde domeinen te waarborgen en om mogelijke additionele informatiebeveiligingsrisico's die door de decentralisatie kunnen ontstaan voor gemeenten en partners te verminderen. Deze additionele risico's moeten worden geanalyseerd. Om de informatiebeveiligingsrisico's te verminderen dienen passende maatregelen te worden geselecteerd die genomen moeten worden bij gemeenten, op knooppunten, op koppelvlakken en bij en/of door leveranciers. De maatregelen kunnen technisch, procedureel, organisatorisch of beleidsmatig van aard zijn (integraliteit) en dienen aan te sluiten bij het niveau van gevoeligheid en de kwetsbaarheid van de informatie.

Om de informatiebeveiliging met betrekking tot de drie decentralisaties adequaat in te richten is het van belang om inzicht te krijgen in de noodzakelijke informatievoorziening, de gegevensuitwisseling en ICT-voorzieningen en de afhankelijkheden te analyseren. Hierbij zullen gesprekken over de informatievoorziening en toepassing van ICT met gemeenten, departementen en andere betrokkenen gevoerd dienen te worden. Tijdens deze gesprekken zal inzicht verkregen moeten worden in onder andere:

- Welke processen noodzakelijk zijn?
- Welke informatiesystemen deze processen ondersteunen?
- Welke gegevens hierbij noodzakelijk zijn?
- Welke informatiestromen plaatsvinden?
- Tussen welke partijen (welke) gegevens worden uitgewisseld?
- Wie welke gegevens mag inzien, wijzigen en (eventueel) verwijderen?
- Welke rollen worden onderkend?
- Waar en hoe de gegevens worden bewaard?
- Wie het beheer over de ICT uitvoert? Denk hierbij aan: de gemeente, departement, ketenpartners of is dit uitbesteed.

1.3 Hoe te lezen

Afhankelijk van de informatiebeveiligingsrisico's en de door de gemeente gemaakte inrichtingskeuzes voor de drie decentralisaties zijn mogelijk additionele specifieke maatregelen nodig ten opzichte van de BIG. Om gemeenten handvatten te bieden welke relevante documenten kunnen worden gebruikt om informatiebeveiliging vanaf het begin mee te nemen wordt een koppeling gelegd met de aandachtspunten vanuit de decentralisaties.

In dit document wordt een overzicht gegeven van (operationele) documenten die gemeenten helpen bij de implementatie van de beveiligingsmaatregelen. Uiteraard is hierbij de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG) het uitgangspunt.

Structuur

De indeling van dit document is als volgt:

Hoofdstuk 1 geeft de algemene inleiding over de Informatiebeveiligingsdienst en informatiebeveiliging in relatie tot de decentralisaties.

Hoofdstuk 2 gaat kort in op het programma van eisen, de verschillende Archetype en Thema's.

Hoofdstuk 3 geeft een uitgebreidere beschrijving van informatieveiligheid in het sociale domein.

Hoofdstuk 4 gaat in op de verschillende organisaties die een belangrijke rol spelen op het gebied van informatieveiligheid. Tevens wordt per organisatie een overzicht gegeven van de producten op het gebied van informatiebeveiliging die door deze organisaties zijn of op korte termijn worden gepubliceerd.

Hoofdstuk 5 geeft een overzicht van relevante informatiebeveiligingsonderwerpen en een koppeling van de deze onderwerpen met de producten van de verschillende producten uit hoofdstuk 4.

2 Programma van eisen

2.1 inleiding

Gemeenten zijn op zoek naar ICT-voorzieningen en systemen die hun werk kunnen ondersteunen. De markt confronteert gemeenten met hun oplossingen. Het verwerven van een systeem is alleen zinnig als de gemeente weet waaraan een systeem minimaal moet voldoen. Het opstellen van een programma van eisen (PvE) helpt gemeente hierbij. In dit PvE worden de functionele eisen en wensen en niet functionele eisen (non functional requirements) voor een ICT-voorziening in het sociaal domein beschreven. Het is hiermee niet gezegd dat de uiteindelijke ICT-voorziening en inrichting hiervan exact aan moet voldoen, maar het is wel de bedoeling dat de ICT-voorziening qua functionaliteiten zoveel mogelijk elementen bevat en zoveel mogelijk voldoet aan de niet functionele eisen.

Inzet van ICT

Informatie en ICT zijn onmisbaar om deze decentralisaties te laten slagen. Het is van belang dat alle bij de decentralisaties betrokken partijen – de gemeenten voorop – zich een beeld vormen van de toekomstige informatievoorziening in het sociaal domein.

De inzet van ICT en informatievoorziening is geen doel op zich, maar ondersteunen op efficiënte wijze een effectieve uitvoering. Dit bespaart kosten en helpt de administratieve lasten te reduceren. Informatievoorziening is verder van belang voor de verantwoording, beleidsinformatie, de (proces)sturing, het toezicht op de kwaliteit en de monitoring van resultaten en effecten. Tenslotte kan ICT helpen om innovaties door te voeren en nieuwe vormen van dienstverlening mogelijk te maken. Een onzekerheid is wel hoe de informatievoorziening in deze nieuwe uitvoeringspraktijk er uit komt te zien.

2.2 Archetype

Een archetype is een geïdealiseerd oermodel dat ten grondslag ligt aan latere varianten. Een archetype is dus een model. Een model past nooit helemaal en er zullen dan ook altijd variaties binnen een model zijn. Natuurlijk zullen er per gemeente verschillende variaties ontstaan. Wel is het zo dat er een duidelijk onderscheid te zien is tussen de typen. De volgende archetypes worden onderscheiden:

- Archetype 1 Transitie-proof.
- Archetype 2 Totaal
- Archetype 3 Geclusterd integraal
- Archetype 4 Integraal in 2e instantie
- Archetype 5 Geclusterde integraliteit elders

Meer informatie met betrekking tot bovenstaande archetypen is te vinden op de website <http://www.visd.nl/>

2.3 Thema's

Per archetype zal aan verschillende thema's aandacht (invulling) moeten worden gegeven. Het gaat hierbij om de volgende thema's:

- Signalering en melding
- Registratie en Zaakgericht werken
- Informatieveiligheid
- Sturing & bekostiging

Meer informatie met betrekking tot bovenstaande thema's is te vinden op de website <http://www.visd.nl/>

2.4 Belang thema informatieveiligheid

De komende decentralisaties bieden gemeenten de mogelijkheid om de dienstverlening beter, integraler en meer in samenhang te organiseren, maar dit moet natuurlijk wel veilig gedaan worden. Goed en zorgvuldig gegevensdelen in het sociale domein vraagt namelijk ook aandacht van een goede beveiliging die betrekking heeft op processen & organisatie, kennis & bewustwording en gedrag.

Dit thema biedt gemeenten handreikingen om hun informatie en informatieprocessen adequaat te beveiligen. Informatieveiligheid en het waarborgen van privacy zijn aspecten die zich niet beperken tot het sociale domein maar die gemeentebreed in vrijwel de gehele dienstverlening een belangrijke rol spelen.

2.5 Uitwisseling (persoons)gegevens binnen het sociale domein

Door de decentralisaties zullen gemeenten meer persoonsgegevens van burgers gaan verwerken. Daarbij gaat het onder andere om medische en strafrechtelijke persoonsgegevens. Bovendien zullen gegevens uit het ene sociale domein ook in een ander domein worden gebruikt. Om dit op een adequate manier te kunnen beveiligen zullen de privacyrisico's nauwkeurig in kaart moeten worden gebracht. Een middel om deze risico's en privacywaarborgen van burgers in kaart te brengen is het uitvoeren van een Privacy Impact Assessment (PIA).³

Hierbij is het van belang om te weten uit welke bronnen deze gegevens betrokken kunnen worden, wie is de eigenaar van deze gegevens (broneigenaar) en hoe partijen (gemeenten, ketenpartners en burgers) deze informatie met elkaar kunnen uitwisselen.

Een groot afbreukrisico is dat meer personen informatie van cliënten kunnen raadplegen en muteren dan degenen die daartoe vanuit hun functie geautoriseerd zijn. Hieronder wordt niet een volledig beeld van alle vereisten op het gebied van privacy en informatiebeveiliging geschetst, maar belangrijke aandachtspunten hierbij zijn:

- Inzicht in de (noodzakelijke) processen.
- Inzicht in de noodzakelijke informatiesystemen.
- Inzicht in de noodzakelijke gegevens.
- Inzicht in het Programma van Eisen (PvE).
- Inzicht in de contracten voor de informatiesystemen.
- Autorisatiematrix van bevoegdheden in de systemen.
- Inzicht in de (noodzakelijke) koppelingen tussen de verschillende informatiesystemen.

³ Het College bescherming persoonsgegevens (CBP) dringt bij het Rijk aan om een Privacy Impact Assessment (PIA) uit te voeren die de risico's en privacywaarborgen in kaart brengt (http://www.cbppweb.nl/Pages/pb_20131030_privacyrisico-taken-gemeenten.aspx)

- Inzicht in de informatiebeveiliging.
- Inzicht in de van toepassing zijnde wet- en regelgeving.
- Inzicht in de (relevante) bedreigingen.
- Inzicht in de (relevante) risico's.

Risico's die in de 'Handreiking - Financiën en de 3 decentralisaties' van het ministerie van Binnenlandse Zaken zijn onderkend zijn onderverdeeld in: sociaal inhoudelijk, personeel, juridisch, informatisering, economie / financieel, politiek, organisatie & leiderschap en samenwerking.

Relevante risico's met betrekking tot informatiebeveiliging en privacy zijn:

- Dienstverlening komt niet op het gewenste niveau. (Sociaal inhoudelijk)
- Betrokken medewerkers implementeren de gewenste planning & controle maatregelen onvoldoende. (Personeel)
- Hulpverleners krijgen privégegevens onder ogen. (Juridisch)
- Het werkproces (en de daarvoor gebouwde ICT) blijkt strijdig met de Wet Bescherming Persoonsgegevens (Wbp). (Juridisch)
- De proeftuinen gaan van start zonder duidelijkheid over (on)mogelijkheden vanwege privacywetgeving. (Juridisch)
- De privacy is onvoldoende geborgd in de manier waarop de systemen worden ingericht en bijhorende handelswijze. (Juridisch)
- De inkoopcontracten blijken juridische onjuistheden te bevatten. (Juridisch)
- De ICT-voorziening voldoet niet aan de gewenste kwaliteit. (Informatisering)
- De gemeente slaagt er niet in om per 1 januari 2015 goed werkende automatiseringssystemen te implementeren. (Informatisering)
- De planning & controlcyclus prioriteert de werkzaamheden verkeerd. (Economie / financieel)
- Het kwaliteitsniveau lijdt te veel onder de aandacht voor het budget. (Economie / financieel)
- De afstemming met ketenpartijen en concernpartijen is onvoldoende. Ketenpartijen hebben meer invloed op projectresultaten dan vooraf gedacht. (Samenwerking)

Juridisch kader

Gegevens, die de gemeenten en zorgaanbieders in hun dossiers registreren, hebben veelal een medische of justitiële achtergrond. De organisatorische en technische beveiliging van de gegevens, en de bescherming van de privacy van de betrokkenen is van absoluut belang.

Er zal een gedegen juridisch kader moeten komen die de gegevensuitwisseling over de verschillende deeldomeinen mogelijk maakt, tezamen met een helder afwegingskader over wat wel en niet is toegestaan ten behoeve van één gezin, één plan, één regie.

Voor uitwisseling van persoonsgegevens is dan ook een wettelijke basis vereist. Bijvoorbeeld tussen bestuursorganen en uitvoeringsinstanties. Bij deze samenwerkingsverbanden moet steeds goed inzichtelijk zijn wie de verantwoordelijke⁴ en wie de bewerker⁵ van persoonsgegevens is. De richtlijnen van het College Bescherming Persoonsgegevens (CBP) over Informatie delen in samenwerkingsverbanden zijn hierbij leidend.

⁴ De verantwoordelijke in de zin van de Wbp is degene die het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt (Artikel 1 sub d). De verantwoordelijke bepaalt welke persoonsgegevens, voor welk doel, op welke manier en met welke middelen worden verwerkt.

⁵ Bij de verwerking van persoonsgegevens kan de verantwoordelijke een bewerker inschakelen. De bewerker is een buiten de organisatie van de verantwoordelijke staande persoon of instelling. Hij bewerkt gegevens ten behoeve van de verantwoordelijke, dat wil zeggen overeenkomstig diens instructies en onder diens (uitdrukkelijke) verantwoordelijkheid. De bewerker beperkt zich tot het verwerken van persoonsgegevens zonder zeggenschap te hebben over het doel van en de middelen voor de verwerking van persoonsgegevens. Hij neemt geen beslissingen over het gebruik van de gegevens, de verstrekking aan derden en andere ontvangers, de duur van de opslag van de gegevens enz.

Bij iedere gegevensuitwisseling zullen (in het kader van de Wbp) de volgende vragen beantwoord moet worden:

- Welke gegevens worden in welke situaties tussen welke partijen uitgewisseld?
- Wat is het doel van die uitwisseling?
- Waarom is de uitwisseling noodzakelijk? Houdt hierbij rekening met proportionaliteit.
- Wie is de gegevenseigenaar?
- Wie is de bewerker?

3 Informatieveiligheid

3.1 Wat is informatieveiligheid?

Door de toenemende digitalisering is het zorgvuldig omgaan met de informatie en gegevens van burgers en organisaties ook voor gemeenten van groot belang. Uitval van computers of telecommunicatiesystemen, het in ongerede raken van gegevensbestanden of het door onbevoegden kennismaken dan wel manipuleren van bepaalde gegevens kan ernstige gevolgen hebben voor de continuïteit van de bedrijfsvoering en het primaire proces. Een betrouwbare, beschikbare en correcte informatiehuishouding is essentieel voor de dienstverlening van gemeenten. Het is niet ondenkbaar dat hieraan ook politieke consequenties verbonden zijn of dat het imago van de gemeente en daarmee van de overheid in het algemeen wordt geschaad. Om informatieveiligheid (doel) te waarborgen wordt gebruik gemaakt van informatiebeveiliging (maatregel).

Informatiebeveiliging is de verzamelnaam voor de processen, die ingericht worden om de betrouwbaarheid van gemeentelijke processen, de gebruikte informatiesystemen en de daarin opgeslagen gegevens te beschermen tegen al dan niet opzettelijk incidenten. Binnen het vakgebied informatiebeveiliging wordt onderscheid gemaakt tussen beschikbaarheid, integriteit, vertrouwelijkheid en controleerbaarheid.

- **beschikbaarheid:** het zorg dragen voor het beschikbaar zijn van informatie en informatie verwerkende bedrijfsmiddelen (informatiesystemen) op de juiste tijd en plaats voor de gebruikers. Hierdoor hebben burgers en bedrijven toegang tot voor hen relevante informatie en hebben medewerkers toegang tot relevante informatie om hun werk en hun dienstverlening richting onze burgers en bedrijven ongestoord voort te zetten.
- **integriteit:** het waarborgen van de correctheid, volledigheid, tijdigheid (actualiteit) en controleerbaarheid van informatie en informatieverwerking. Voor een efficiënte en effectieve bedrijfsvoering is het voor de gemeente van belang dat de correcte informatie tijdig aanwezig is in de systemen. Maar ook dat zelfs na een bepaalde periode de correctheid en de volledigheid van informatie eenvoudig gecontroleerd kan worden (=controleerbaarheid).
- **vertrouwelijkheid:** het beschermen van informatie tegen kennisname en mutatie door onbevoegden. Informatie is alleen toegankelijk voor degenen die hiertoe geautoriseerd zijn.
- **controleerbaarheid:** de mogelijkheid om met voldoende zekerheid vast te kunnen stellen of wordt voldaan aan de eisen ten aanzien van beschikbaarheid, integriteit en vertrouwelijkheid.

3.2 Veiligheid, privacy en beveiliging in het kader van 3D

Voor het ondersteunen van de eigen kracht krijgt de burger toegang tot zijn of haar (gezins)dossier. Met behulp van deze 'toegang' kan de burger waar en wanneer mogelijk zelf regie voeren. Desgewenst kan een mantelzorger door de burger gemachtigd worden van deze toegang gebruik te maken (bijvoorbeeld aan zelf afspraken plannen en combineren en het voeren van persoonlijk budgetbeheer). De burger ziet welke ondersteuning wordt gegeven en welke informele zorg wordt georganiseerd door zijn/haar sociale omgeving. De burger ziet welke informatie over hem/haar/het gezin uitgewisseld wordt tussen de gemeente en de tweedelijns ondersteuners (inkijk).

Voor de regierol van de gemeente bij multiprobleemgezinnen is een totaaloverzicht van alle betrokken ondersteuners (professionele én informele zorg) nodig in de vorm van de registratie van één plan. Voor de regierol is het tevens noodzakelijk dat de regisseur de voortgang van de hulpverlening bewaakt en er met de diverse ondersteuners (professioneel en informeel) en de burger kan worden gecommuniceerd (berichtgeving). Deze communicatie kan gestructureerd (verstrekking start dienstverlening, ketenbericht) of ongestructureerd (bijvoorbeeld stellen en beantwoorden van een vraag) plaatsvinden.

Persoonsgegevens in de zin van de Wet Bescherming Persoonsgegevens (Wbp) zijn alle gegevens betreffende een geïdentificeerde of identificeerbare natuurlijke persoon. Een persoon is identificeerbaar indien zijn identiteit redelijkerwijs, zonder onevenredige inspanning, vastgesteld kan worden.

Privacy en beveiliging

Privacy en beveiliging zijn zeer belangrijke uitgangspunten voor de te organiseren informatievoorziening. Het gaat immers om vertrouwelijke informatie over mensen in kwetsbare situaties.

Zowel voor alle informatie-uitwisseling tussen professionals als ook voor de inblikfunctionaliteit door de burger (inzage in het eigen dossier) geldt dat privacy voorop staat. Ongeoorloofde toegang door derden tot bijvoorbeeld het dossier (doordat men zich voordoeft als de burger zelf) moet te allen tijde voorkomen worden. Dit vraagt niet alleen om strenge beveiliging in de zin van autorisaties op het dossier, het vereist met name aandacht voor de organisatorische kant van de informatiebeveiliging en voor een sluitende identificatie/authenticatie van de burger voor de toegang tot het systeem.

Dit geldt ook voor de regisseur, professional en/of medewerker, zeker als die in het veld toegang moeten hebben tot nog meer informatie dan de burger zelf.

Zowel bij regievoering als voor de informatiehuishouding moet rekening worden gehouden met reguliere trajecten (uitgangspunt: de burger zelf kan veel inzien, eventueel kan corrigeren; hij/zij heeft het heft zelf in handen) en trajecten waar sprake is van dwang (waar de burger veelal zelf veel minder inzage en geen correctierecht zal of mag hebben in het eigen dossier).

Opdrachtverstrekking

Bij de opdrachtverstrekking is het belangrijk dat gemeenten de privacy en informatiebeveiliging borgen. Daarom raden wij aan om bij uit- of aanbesteding van gegevensverwerking aan een private partij contractuele afspraken te maken over⁶:

- Continuïteit van dienstverlening.
- Ondernemingsrechtelijke structuur met het oog op voorkoming van doorgifte van persoonsgegevens aan derde landen.
- Het niveau van informatiebeveiliging.

⁶ zoals artikel 14, lid 2 Wpb voorschrijft (<http://www.cbppweb.nl/wbpnaslag/2/Paginas/wbp-artikel-14-2.aspx>).

4 Organisaties in het kader van informatieveiligheid

Er zijn verschillende organisaties die een belangrijke rol spelen op het gebied van informatieveiligheid. Hieronder wordt een overzicht gegeven van die organisaties die van belang zijn in het kader van 3D. Tevens wordt per organisatie een overzicht gegeven van de producten op het gebied van informatiebeveiliging die door deze organisaties zijn of worden gepubliceerd.

4.1 Informatiebeveiligingsdienst voor gemeenten

De Informatiebeveiligingsdienst voor gemeenten (IBD)⁷ is een gezamenlijk initiatief van de Vereniging van Nederlandse Gemeenten (VNG) en het Kwaliteitsinstituut Nederlandse Gemeenten (KING) en actief sinds 1 januari 2013. De IBD is er voor alle gemeenten en richt zich op bewustwording en concrete ondersteuning om gemeenten te helpen hun informatiebeveiliging naar een hoger plan te tillen.

Hieronder volgt een overzicht van de relevante documenten die door de IBD zijn of worden gepubliceerd. Deze documenten zijn beschikbaar op de (publieke) website⁸ en de community site⁹ van de IBD. Ook toekomstige documentatie zal hier worden gepubliceerd.

Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG)

Het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties (BZK) heeft opdracht gegeven voor het ontwikkelen van een Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG). De Baseline Informatiebeveiliging Nederlandse Gemeenten is bedoeld om:

1. Gemeenten op een vergelijkbare manier efficiënt te laten werken met informatiebeveiliging.
2. Gemeenten een hulpmiddel te geven om aan alle eisen op het gebied van Informatiebeveiliging te kunnen voldoen.
3. De auditlast bij gemeenten te verminderen.
4. Gemeenten een aantoonbaar betrouwbare partner te laten zijn.

Met deze baseline hebben bestuur en management van gemeenten een instrument in handen waarmee zij in staat zijn om te meten of de eigen organisatie 'in control' is op het gebied van informatiebeveiliging. Deze baseline is vervaardigd op basis van de Baseline Informatiebeveiliging Rijksdienst (BIR) voor de gemeentelijke markt. Het betreft twee varianten: een Strategische- én een Tactische Baseline.

- De Strategische Baseline¹⁰ kan gezien worden als de 'kapstok' waaraan de elementen van informatiebeveiliging opgehangen kunnen worden. Centraal staan de organisatie en de verantwoording over informatiebeveiliging binnen de gemeente.
- De Tactische Baseline¹¹ beschrijft de normen en maatregelen ten behoeve van controle en risicomanagement. De Tactische Baseline beschrijft aan de hand van dezelfde indeling als de

⁷ <http://new.kinggemeenten.nl/informatiebeveiliging>

⁸ <http://new.kinggemeenten.nl/informatiebeveiliging/downloads-informatiebeveiligingsdienst>

⁹ <https://new.kinggemeenten.nl/informatiebeveiliging/ib-community>

¹⁰ http://new.kinggemeenten.nl/sites/default/files/document/gr_1891/Strategische-Baseline-Informatiebeveiliging-Nederlandse-Gemeenten-mei-2013-versie-1.0-IBD.pdf

¹¹ http://new.kinggemeenten.nl/sites/default/files/document/gr_1891/Tactische-Baseline-Informatiebeveiliging-Nederlandse-Gemeenten-mei-2013-versie1.0-IBD.pdf

internationale beveiligingsnorm ISO/IEC 27002:2007, de controls/maatregelen die als baseline gelden voor de gemeenten.

Operationele producten BIG

Op basis van de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG) ontwikkelt de Informatiebeveiligingsdienst voor gemeenten (IBD) operationele producten behorend bij de BIG. Met behulp van deze operationele producten kan iedere gemeente tot implementatie van de BIG overgaan. De IBD ontwikkelt deze operationele producten in samenwerking met de Taskforce BID en een groot aantal betrokken gemeenten die de producten reviewen voordat ze definitief worden.

De volgende operationele producten BIG zijn door de IBD gepubliceerd:

Aanwijzing Logging: Het doel van dit document is een aanwijzing te geven over het gebruik van logging binnen gemeentelijke systemen.

Anti-malware beleid: Dit document geeft een mogelijke invulling van beleidsuitgangspunten voor het Anti-malware beleid weer. Deze beleidsuitgangspunten zijn afkomstig uit de BIG en het beleid is daarmee compliant aan de BIG.

Back-up en Recovery Gemeente: Het doel van dit document is een aanwijzing te geven over hoe het back-up en recovery beleid van een gemeente opgezet en uitgevoerd kan worden.

Bewerkersovereenkomst: Dit product bevat een standaard bewerkersovereenkomst en een voorbeeld bijlage met maatregelen voor de bewerker die de gemeente als verantwoordelijke kan gebruiken bij het laten bewerken van persoonsgegevens.

Cloud Computing: Dit document geeft uitgangspunten weer, gezien vanuit informatiebeveiliging, voor een invulling van het Cloud Computing beleid voor gemeenten. Deze beleidsuitgangspunten informatiebeveiliging zijn afkomstig uit de BIG en het beleid is daarmee compliant aan de BIG.

GAP-analyse: Het doel van de GAP-analyse is om gemeenten te controleren of en in welke mate de maatregelen uit de tactische variant van de BIG zijn geïmplementeerd. Hierbij gaat het om gemeenten die het onderzoek uitvoeren of laten uitvoeren.

Geheimhoudingsverklaringen BIG: Dit product bevat voorbeelden van geheimhoudingsverklaringen, die door de gemeenten te gebruiken zijn. Deze geheimhoudingsverklaringen zijn onderdeel van de BIG.

Handleiding screening personeel: Dit document geeft een handleiding over hoe invulling kan worden gegeven aan de verificatie van de achtergrond voor alle kandidaten (werknemers), ingehuurd personeel en externe gebruikers. Deze verificatie heet ook screening van personeel en wordt al binnen gemeenten gebruikt voor wat betreft het verkleinen van integriteitsrisico's.

Handreiking CISO functieprofiel: Activiteiten voor informatiebeveiliging behoren te worden gecoördineerd door vertegenwoordigers uit de verschillende delen van de organisatie met relevante rollen en functies. De rollen van de Chief Information Security Officer (CISO) en het lijnmanagement zijn beschreven. Bij kleine gemeenten kan deze rol ook in deeltijd uitgevoerd worden, waarbij het ook mogelijk is om dit te combineren over verschillende gemeenten in een regionale opzet.

Handreiking dataclassificatie: Dit document bevat een good practice voor (data)classificatie. Data betekent in dit verband alle gegevens en informatie, ongeacht het medium waarop deze opgeslagen wordt en ongeacht de presentatie daarvan.

Hardening beleid voor gemeenten: Dit document geeft een mogelijke invulling van beleidsuitgangspunten voor het hardening-beleid weer. Deze beleidsuitgangspunten zijn afkomstig uit de BIG en het beleid is daarmee compliant aan de BIG.

Implementatie BIG: Het doel van de 'Implementatie BIG' is om binnen de gemeente te toetsen of en in welke mate de gemeente voldoet aan de maatregelen uit de BIG.

Inkoopvoorwaarden en informatiebeveiligingseisen: Dit product bevat aanwijzingen voor beveiligingseisen in inkoopvoorwaarden van de gemeente.

Mobiele gegevensdragers: Dit product bevat aanwijzingen en beleid rondom het gebruik van mobiele gegevensdragers zoals USB sticks of back-up media.

Mobile Device Management: Er is een toename van het gebruik van mobiele gegevensdragers zoals smartphones, tablets en laptops binnen de gemeenten. Deze aanwijzing is geschreven om vanuit verschillende gezichtspunten de risico's en oplossingen weer te geven die gemeenten kunnen inzetten bij de keuzes voor mobiele apparaten. Ook wordt een lijst met functionele eisen en wensen gegeven voor het geval dat men een MDM-oplossing wil implementeren voor het beheeren van mobiele apparaten en de gemeentelijke gegevens die erop kunnen staan.

Patch management voor gemeenten: Patch Management is het proces waarmee patches op gecontroleerde beheerste (risico beperkende) wijze uitgerold kunnen worden. Patches zijn doorgaans kleine programma's die aanpassingen maken om fouten op te lossen of verbeteringen aan te brengen in bestaande programmatuur en/of hardware. Patch Management wordt meestal uitgevoerd door de ICT-afdeling binnen een organisatie. Het doel van Patch Management is tweeledig. Ten eerste is het gericht op het inzichtelijk maken van de actuele stand van kwetsbaarheden en toegepaste patches binnen de beheerde infrastructuur. Het tweede doel is op een zo efficiënt en effectief mogelijke wijze met zo min mogelijk verstoringen stabiele (veilige) systemen te creëren en te houden.

Presentatie Bewustwording Informatieveiligheid bij gemeenten: De presentatie is bedoeld voor iedere medewerker binnen de gemeente. Met als doel om alle medewerkers bewust te maken van de informatiebeveiligingsrisico's die de gemeente loopt en ook van de wijze waarop zij zich hiertegen kan beschermen. Elke gemeente kan de presentatie overigens aanpassen naar de eigen gemeentelijke situatie. De BIG en het Informatiebeveiligingsbeleidsplan, ook een operationeel product van de BIG, zijn als uitgangspunt genomen voor de presentatie.

Responsible Disclosure: In de ICT-wereld bestaan meerdere praktijken om kwetsbaarheden in ICT bekend te maken. Responsible Disclosure binnen de ICT-wereld is het op een verantwoorde wijze, en in gezamenlijkheid tussen melder en organisatie, openbaar maken van ICT-kwetsbaarheden op basis van een, door organisaties hiervoor, vastgesteld beleid voor Responsible Disclosure. Dit document geeft een template weer voor het beleid op het vlak van Responsible Disclosure, waarin een aantal aspecten standaard is opgenomen, zoals het delen van de meldingen met de IBD.

Toegangsbeleid: Dit document bevat een good practice voor het toegangsbeleid van een gemeente. De in deze handreiking genoemde niveaus en (bewaar)termijnen zijn een voorstel en komen uit verschillende brondocumenten. Waaronder: wetgeving, PVIB-patronen, een gemeente en de Strategische deel van de BIG.

Voorbeeld Incident Management en responsebeleid: Dit document geeft een mogelijke invulling van beleidsuitgangspunten voor het Incident Management en Responsebeleid weer en aanwijzingen voor gebruik en inrichting van een Incident Management en responseteam. Deze beleidsuitgangspunten zijn afkomstig uit de BIG en het beleid is daarmee compliant aan de BIG.

Voorbeeld Informatiebeveiligingsbeleid Gemeenten: Dit document geeft algemene beleidsuitgangspunten over informatiebeveiliging van de gemeente.

Wachtwoordbeleid: Dit product bevat aanwijzingen en een beleid rondom het gebruik van wachtwoorden binnen de gemeente.

De volgende operationele producten BIG zijn in ontwikkeling:

Uitgebreide risicoanalyse methode: Doelstelling van de uitgebreide risicoanalyse is om in kaart te brengen welke maatregelen aanvullend op de baseline moeten worden getroffen om het juiste niveau van beveiliging te realiseren.

Verkorte risicoanalyse methode: Het doel van dit document is het leveren van een aanpak die gebruikt kan worden om voor nieuwe processen en systemen een methode te hebben om te bepalen of de BIG afdoende is of niet. Tevens kan deze aanpak ook gebruikt worden om bij een bestaand systeem te toetsen of deze voldoende beveiligd is door de BIG maatregelen.

Contractmanagement: Het doel van dit document is aanwijzingen te geven omtrent contractmanagement.

Encryptiebeleid (PKI): Deze handleiding is geschreven om vanuit verschillende gezichtspunten de risico's en oplossingen weer te geven die gemeenten kunnen inzetten rondom encryptie/versleuteling en Public Key Infrastructure (PKI).

Handreiking communicatieplan gemeente: Deze aanwijzing is geschreven om vanuit verschillende gezichtspunten de risico's en oplossingen weer te geven die gemeenten kunnen inzetten rondom telewerken.

Handreiking proces configuratiebeheer: Dit product bevat aanwijzingen voor het omgaan van alle componenten die deel uitmaken van de ICT-infrastructuur, en aanwijzingen voor gebruik en inrichting van het proces configuratiebeheer.

Handreiking Wijzigingsbeheer: Dit product bevat aanwijzingen voor het omgaan met het doorvoeren van wijzigingen in de ICT-middelen en -diensten, en aanwijzingen voor gebruik en inrichting van het proces wijzigingsbeheer.

Logische toegangsbeveiliging: Dit product bevat aanwijzingen en een beleid rondom het inrichten van logische toegangsbeveiliging binnen de gemeente.

Procedure Afvoer ICT middelen: Dit product bevat aanwijzingen voor het omgaan met het afvoeren van IT middelen.

Procedure nieuwe ICT-voorzieningen: Dit product bevat aanwijzingen voor het vastleggen van de verschillende stappen die noodzakelijk zijn om nieuwe versies, releases of updates van ICT-voorzieningen goed te keuren alvorens deze in productie worden genomen.

Telewerken beleid: Deze aanwijzing is geschreven om vanuit verschillende gezichtspunten de risico's en oplossingen weer te geven die gemeenten kunnen inzetten rondom telewerken.

Toelichting bij het Privacy Impact Assessment (PIA): Dit document is de toelichting bij het Privacy Impact Assessment (PIA) instrument ter ondersteuning bij het uitvoeren van de PIA.

4.2 Nationaal Cyber Security Centrum (NCSC)

Het Nationaal Cyber Security Centrum (NCSC)¹² draagt bij aan het gezamenlijk vergroten van de weerbaarheid van de Nederlandse samenleving in het digitale domein en daarmee aan een veilige, open en stabiele informatiesamenleving door het leveren van inzicht en het bieden van handelingsperspectief. De primaire doelgroepen van het NCSC zijn Rijksoverheid en organisaties in de vitale infrastructuur. Het centrum valt organisatorisch onder de Nationaal Coördinator Terrorismedebestrijding en Veiligheid (NCTV) van het ministerie van Veiligheid en Justitie maar is gestoeld op publiek-private samenwerking.

Gedegen kennis over de aard, urgentie en gevolgen van cyber crime is belangrijk om goede maatregelen te kunnen nemen. Het Nationaal Cyber Security Centrum (NCSC) publiceert kennisdocumenten zoals het Cyber Security Beeld Nederland en het Trendrapport Cybercrime en Digitale Veiligheid die gericht zijn op het informeren van hogere bestuurslagen in (vitale) organisaties, publiek en privaat. We publiceren ook uitgaven die specifiek bestemd zijn voor managers en bijvoorbeeld ICT-experts.

¹² <https://www.ncsc.nl/>

Wifi-beveiliging - De onderschatte schakel in netwerkbeveiliging: Draadloos werken biedt vele voordelen maar kent – zeker in vergelijking met een netwerk met vaste aansluitingen – ook ernstige en specifieke dreigingen, die de betrouwbaarheid van de informatievoorziening van een organisatie kunnen aantasten. Deze whitepaper brengt relevante informatie rondom de beveiliging van wifinetwerken in samenhang bij elkaar.

Beveiligingsrichtlijnen voor mobiele apparaten: Het toenemende gebruik van slimme mobiele apparaten biedt veel nieuwe mogelijkheden, maar er kleven ook risico's aan. Daarom publiceert het Nationaal Cyber Security Centrum (NCSC) richtlijnen voor de beveiliging van mobiele apparaten.

Consumerization en security: Slimme mobieltjes, data in 'de cloud' en altijd online: de manier waarop we ICT gebruiken is structureel veranderd. De opkomst van de tablets, smartphone's en slimme clouddiensten benadrukken dit. Dit consumentgedreven gebruik van ICT (consumerization) brengt beveiligingsrisico's met zich mee.

ICT-beveiligingsrichtlijnen voor webapplicaties: De ICT- beveiligingsrichtlijnen voor webapplicaties vormen een leidraad voor het veiliger ontwikkelen, beheren en aanbieden van webapplicaties en bijbehorende infrastructuur. De beveiligingsrichtlijnen zijn breed toepasbaar voor ICT- oplossingen die gebruik maken van webapplicaties. Hierdoor zijn ze zowel door afnemers, als door dienstaanbieders te gebruiken voor aan- en uitbestedingen, toezicht en onderlinge afspraken.

Cloudcomputing: Deze publicatie geeft informatie over cloudcomputing en mogelijke risico's ervan. Met andere woorden: als een organisatie kiest voor 'cloudcomputing', zijn er dan risico's voor de bedrijfsvoering en heeft deze keuze gevolgen voor de informatiebeveiliging van de organisatie?

Responsible Disclosure: Dit dossier bevat de leidraad Responsible Disclosure, voorbeelden van Responsible Disclosure beleid en voorbeelden van Responsible Disclosure.

De documentatie is beschikbaar op de (publieke) website van het NCSC.¹³

4.3 Taskforce Bestuur en Informatieveiligheid Dienstverlening

De Taskforce Bestuur en Informatieveiligheid Dienstverlening (BID)¹⁴ is ingesteld om het onderwerp informatieveiligheid hoog op de agenda te krijgen bij bestuurders en topmanagement van alle overheidslagen. Zowel qua bewustwording als sturing. De Taskforce BID bouwt voort op de huidige initiatieven op informatieveiligheidsvlak vanuit een intensieve samenwerking met de koepelorganisaties van elk van de overheidslagen.¹⁵ Bovendien wordt nauw samengewerkt met betrokken organisaties op informatieveiligheidsvlak, zoals het Nationaal Cyber Security Centrum (NCSC), het Centrum Informatiebeveiliging en Privacybescherming (CIP), de Informatiebeveiligingsdienst voor gemeenten (IBD), het Waterschapshuis en Logius. Doel van de Taskforce Bestuur en Informatieveiligheid Dienstverlening is om uiteindelijk te komen tot verplichtende zelfregulering per overheidslaag als het gaat om informatieveiligheid.

De volgende producten zijn door de Taskforce BID gepubliceerd:

Opleidingsaanbod: Het spoor 'leren' richt zich met name op de verandering in kennis, houding en vaardigheden bij bestuur en management.¹⁶

¹³ <https://www.ncsc.nl/dienstverlening/expertise-advies/kennisdeling>

¹⁴ <http://www.taskforcebid.nl/>

¹⁵ Betrokken koepelorganisaties zijn de Unie van Waterschappen, Interprovinciaal Overleg (IPO), Manifestgroep, Vereniging van Nederlandse Gemeenten (VNG) en Interdepartementale Commissie Chief Information Officers (ICCIO).

¹⁶ <http://www.taskforcebid.nl/producten/het-spoor-leren/>

Zelftest Informatieveiligheid: De Taskforce BID heeft voor u een online test ontwikkeld waarmee u in tien minuten zelf eenvoudig uw kennis en bewustzijn toetst op het gebied van informatieveiligheid. Onderwerpen die aan bod komen gaan over de verschillende aspecten van informatieveiligheid, verantwoordelijken bij informatieveiligheid, informatieveiligheid en ketens, sturen op informatieveiligheid en risicobewustzijn. Met de Zelftest Informatieveiligheid krijgt u een beter beeld van de verschillende aspecten van informatieveiligheid en hoe u daar als bestuurder of topmanager op kunt sturen.¹⁷

De documentatie is beschikbaar op zowel de (publieke) website¹⁸ als de (besloten) Pleio site¹⁹ van de Taskforce BID.

4.4 Centrum voor Informatiebeveiliging en Privacybescherming

Het Centrum voor Informatiebeveiliging en Privacybescherming (CIP)²⁰ is het expertisecentrum voor informatiebeveiliging en privacybescherming van, voor en door overheidsorganisaties. Het CIP is opgericht door vier grote uitvoeringsorganisaties en ZBO's die uitkeringen doen aan burgers: Belastingdienst, DUO, SVB en UWV, waarbij de laatste als trekker optreedt. Kennis die bij de overheidsorganisaties aanwezig is op het vlak van informatiebeveiliging en privacybescherming, wordt binnen de samenwerking in het CIP gebundeld en toegankelijk gemaakt.

Good practices

CIP heeft vier categorieën geformuleerd waarmee de reikwijdte van good practices wordt aangegeven:

1. Individuele praktijk: een toepassing bij een van de organisaties die werkt, als handreiking voor hergebruik binnen geïnteresseerde organisaties. Een individuele praktijk is al bruikbaar nadat een individuele organisatie die aanreikt.
2. Becommentarieerde praktijk: een door meerdere professionals veralgemeniseerde praktijk als handreiking voor hergebruik binnen geïnteresseerde organisaties. Een becommentarieerde praktijk ondergaat eerst een reviewslag binnen een CIP-domeingroep en/of door de CIP-Leesgroep.
3. Gecommitteerde praktijk: een namens meerdere in CIP samenwerkende organisaties onderschreven praktijk, als sterk advies voor hergebruik bij alle organisaties binnen de uitvoerende overheid. Een praktijk is pas gecommitteerd als bestuurders daarvoor hebben gekozen.
4. Verplichtende praktijk: een praktijk die door de in CIP samenwerkende organisaties is bekrachtigd als basis voor zelfregulering binnen deze kring en met een sterk advies om dat voor de gehele overheidslaag van de uitvoering toe te passen. Een praktijk is pas verplichtend als bestuurders daarvoor hebben gekozen.

De volgende producten zijn in de reeks "uit de praktijk" door CIP gepubliceerd:

Grip op Secure Software Development: Organisaties hebben nog onvoldoende vat op security, getuige de explosieve groei van incidenten. In de praktijk blijkt dat 75% van die incidenten hun oorzaak vinden in softwarefouten.

¹⁷ <https://informatieveiligheidstest.nl>

¹⁸ <http://www.taskforcebid.nl>

¹⁹ <https://informatieveiligheid.pleio.nl/>

²⁰ <http://www.cip-overheid.nl/>

- De methode “Grip op secure software development (SSD)” beschrijft hoe een opdrachtgever grip krijgt op het ontwikkelen van goed beveiligde software. De drie pijlers daarbij zijn 1) standaard beveiligingseisen, 2) contactmomenten en 3) inrichten van SSD processen.
- De beveiligingseisen die de opdrachtgever kan hanteren als eisen aan de op te leveren software, zijn vervat in het tweede document.

Borging awareness informatiebeveiliging: Dit product bestaat uit een presentatie en bijbehorende verdiepingsmateriaal. “Borging” duidt hier op het proces van voortdurende inspanning om de organisatie bij de les te krijgen en houden op het gebied van informatiebeveiligingsbewustzijn.

Responsible Disclosure - handreiking voor implementatie: ‘Responsible Disclosure’ betreft het op verantwoorde wijze melden van ICT-kwetsbaarheden, op basis van een protocol dat de organisatie en de ontdekker van de kwetsbaarheid duidelijkheid biedt. CIP biedt hiervoor een template voor het beleid en een checklist van acties die nodig zijn om dat te realiseren.

Meldplicht Datalekken en meldplicht Inbreuken op elektronische systemen: Er is wetgeving in de maak die organisaties verplicht inbreuken op ICT systemen – en verlies van persoonsgegevens in het bijzonder – onverwijld te melden bij respectievelijk het ministerie van Veiligheid en Justitie, annex het Nationaal Cyber Security Centrum (NCSC) en het College Bescherming Persoonsgegevens annex de getroffen burgers. Nalatigheid kan hoge boetes opleveren. Op Europese schaal is soortgelijke wetgeving op handen, die er qua consequenties nog een flinke schep bovenop doet. Hoe verhouden deze zaken zich tot elkaar en wat u zoal moet organiseren om aan de nieuwe verplichtingen te kunnen voldoen?

Testen met persoonsgegevens: Het doel van dit document is om beveiligingsgerelateerde richtlijnen te geven voor het gebruik van persoonsgegevens in testsituaties buiten de productieomgeving. Het document is in lijn met de gangbare algemene baselines, normenkaders en best practices, met name de ISO 27xxx normen, de Code voor Informatiebeveiliging, en het tactisch normenkader van de Baseline Informatiebeveiliging Rijksdienst (BIR-TNK) voor zover van toepassing.

Beveiligingsbeleid clouddiensten: Het bespreekt de relatie van verschillende cloudtypes met de diverse aspecten van informatiebeveiligingsbeleid. Het resultaat is een checklist van opletpunten (vereisten zo je wilt) bij het inzetten van clouddiensten.

Privacy impact assessment: De eerdere publicatie op deze plek moesten wij terugtrekken. Nieuwe, praktijkgerichte documentatie rond het thema PIA van de hand van onze kennispartner Considerati wordt op korte termijn op deze plaats beschikbaar gesteld.

De documentatie is beschikbaar op zowel de (publieke) website²¹ als de (besloten) Pleio site²² van het CIP.

4.5 College bescherming persoonsgegevens

Het College bescherming persoonsgegevens (CBP) ²³ houdt toezicht op de naleving van de wettelijke regels die zien op de bescherming van persoonsgegevens, zo nodig met behulp van sancties. Daarnaast adviseert het CBP de regering over voorgenomen wetgeving die betrekking heeft op de verwerking van persoonsgegevens. Bij het uitvoeren en verantwoorden van zijn werkzaamheden heeft het CBP oog voor de maatschappelijke context van de aan hem voorgelegde vragen, problemen of klachten.

²¹ <http://www.cip-overheid.nl/>

²² <http://www.cip-pleio.nl/>

²³ <http://www.cbpreweb.nl/Pages/home.aspx>

De volgende producten zijn door de Taskforce BID gepubliceerd:

Privacy by Design: Organisaties willen zorgvuldig omgaan met de gegevens die hen ter beschikking staan en die hun vaak in vertrouwen zijn verstrekt. Door al tijdens de ontwikkeling van informatiesystemen aandacht te schenken aan privacyverhogende maatregelen (Privacy Enhancing Technologies of PET) kan op een effectieve manier zorgvuldige en verantwoorde omgang met persoonsgegevens technisch worden afgedwongen. Privacy by Design speelt niet alleen een belangrijke rol bij de ontwikkeling van grote ICT-projecten, maar kan ook een rol van betekenis spelen bij de invoering van RFID, het Burgerservicenummer of mobiel betalen.

Richtsnoeren beveiliging van persoonsgegevens: De richtsnoeren leggen uit hoe het CBP bij het onderzoeken en beoordelen van beveiliging van persoonsgegevens de beveiligingsnormen uit de Wet bescherming persoonsgegevens (Wbp) toepast. De richtsnoeren vormen de verbindende schakel tussen het juridisch domein, met daarbinnen de eisen uit de Wbp, en het domein van de informatiebeveiliging, waarin de noodzakelijke kennis en kunde aanwezig is om daadwerkelijk aan die eisen te voldoen.

Compliance-instrumenten: De bescherming van persoonsgegevens is een verantwoordelijkheid voor alle organisaties die met persoonsgegevens omgaan. Het CBP stimuleert daarom zelfregulering van overheid en bedrijfsleven voor een adequate privacybescherming. Het CBP heeft in samenwerking met diverse marktpartijen de afgelopen jaren een viertal compliance-instrumenten ontwikkeld. De samenhang tussen deze instrumenten en het algemene begrippenkader wordt uiteengezet in 'Overzicht van de Zelfreguleringsproducten'.

Medische gegevens: Mensen moeten erop kunnen vertrouwen dat met de medische gegevens die zij toevertrouwen aan een arts, zorgvuldig wordt omgegaan. Medische gegevens zijn per definitie gevoelige gegevens, ook in de zin van de wet. Dit betekent dat ze met de hoogst mogelijke zorgvuldigheid moeten worden verwerkt. Patiënten moeten er absoluut zeker van kunnen zijn dat hun gegevens goed beveiligd zijn en dat onbevoegden geen toegang krijgen tot de gegevens.

Handleiding Wet bescherming persoonsgegevens: Om personen, organisaties, ondernemingen en overheidsinstellingen die persoonsgegevens verwerken of gaan verwerken, behulpzaam te zijn bij het nemen van maatregelen om aan de Wet bescherming persoonsgegevens te voldoen, geeft het ministerie van Justitie deze handleiding uit. Deze handleiding richt zich dus niet tot de burger wiens persoonsgegevens worden verwerkt, maar is bestemd voor de personen, organisaties, ondernemingen en overheidsinstellingen die persoonsgegevens verwerken.

Anonimiseer gegevens bij gebruik big data: Via big data worden op geavanceerde wijze enorme hoeveelheden (persoons)gegevens verwerkt. Het College bescherming persoonsgegevens (CBP) waarschuwt voor de risico's van dit soort gigantische databases en de bijbehorende geautomatiseerde verwerking van persoonsgegevens. Voor veel doelen waarvoor big data wordt ingezet, zijn tot de persoon herleidbare gegevens helemaal niet nodig. De gegevens moeten dan onomkeerbaar worden geanonimiseerd. Als organisaties voor hun doel wél herleidbare gegevens verwerken, moeten zij aan alle eisen van de Wet bescherming persoonsgegevens (Wbp) voldoen.

De documentatie is beschikbaar op de (publieke) website van het CBP.²⁴

4.6 Overige organisaties

Overige organisaties die een rol spelen bij informatieveiligheid zijn de Nederlandse Orde van Register EDP-Auditors (NOREA)²⁵, het National Institute of Standards and Technology (NIST)²⁶ en de International Organization for Standardization (ISO)²⁷ / de NEN (Nederlandse Norm)²⁸.

²⁴ <http://www.cbpweb.nl>

²⁵ <http://www.norea.nl/Norea/Home/default.aspx>

²⁶ <http://www.nist.gov/>

²⁷ <http://www.iso.org/iso/home.html>

²⁸ <http://www.nen.nl/>

5 Aan de slag

Op dit moment is nog niet aangegeven welke documenten voor welke archetype relevant zijn, dit aangezien deze archetypen nog in ontwikkeling zijn. Er is dan ook nog niet goed in te schatten of bepaalde documenten relevanter zijn voor het ene archetype dan wel voor een ander archetype. Op dit moment is vooral de insteek naar specifiek informatiebeveiligingsonderwerp.

5.1 Informatiebeveiligingsonderwerpen

De onderwerpen die op dit moment worden onderkend zijn:

- Inrichten Informatiebeveiliging
- Privacy impact assessment
- Risicoanalyse (inclusief GAP-analyse)
- Beheer ICT-componenten
- Awareness informatiebeveiliging
- Meldplicht Datalekken en meldplicht Inbreuken op elektronische systemen
- Responsible Disclosure
- Authenticatie en Autorisatie (inclusief wachtwoorden)
- Inkopen / aanbesteding
- Secure Software Development
- Persoonsgegevens
- Medische gegevens
- Testen met persoonsgegevens
- Mobiele apparaten en telewerken
- Cloudcomputing
- Big Data

5.2 Ondersteunde documenten

De onderwerpen uit paragraaf 5.1 zijn in tabel 1 verder uitgewerkt. Dit houdt in dat er een koppeling is gelegd tussen de onderwerpen en relevante documenten van diverse organisaties zoals in hoofdstuk 4 benoemd. In hoofdstuk 4 wordt ook een korte omschrijving van de producten waar in tabel 1 wordt gerefereerd.

Onderwerp	CIP	BIG-OP	Overig	Bruikbaar Ja/Nee	Archetype				
					1	2	3	4	5
Inrichten Informatiebeveiliging		<ul style="list-style-type: none"> • Strategische Baseline Informatiebeveiliging Nederlandse Gemeenten mei 2013 versie 1.0 IBD • Tactische Baseline Informatiebeveiliging Nederlandse Gemeenten mei 2013 versie 1.0 IBD • Bijlage hoofdstuk 15.1.1 Identificatie toepasselijke wetgeving • Implementatie BIG • Handreiking CISO functieprofiel • Voorbeeld Informatiebeveiligingsbeleid Gemeenten 	•						
Privacy impact assessment	• Privacy impact assessment bij de Belastingdienst (cip.pleio.nl)	• Toelichting bij het Privacy Impact Assessment (PIA) (in ontwikkeling)	<ul style="list-style-type: none"> • Norea - Handreiking Privacy Impact Assessment • Rijksdienst - Toetsmodel Privacy Impact Assessment (PIA) Rijksdienst 	PIA is een apart project binnen VISD. De output van dit project is wel input voor de risicoanalyse					
Risicoanalyse (inclusief GAP-analyse)		<ul style="list-style-type: none"> • Basis risicoanalyse methode (in ontwikkeling) • GAP-analyse: <ul style="list-style-type: none"> ◦ colofon ◦ resultaat ◦ vragenlijst ◦ uitleg 	•						

Onderwerp	CIP	BIG-OP	Overig	Bruikbaar Ja/Nee	Archetype				
					1	2	3	4	5
Beheer ICT-componenten		<ul style="list-style-type: none"> • Mobiele gegevensdragers • Mobile Device Management • Patch management voor gemeenten • Back-up en Recovery Gemeente • Hardening beleid voor gemeenten • Anti-malware beleid • Aanwijzing Logging • Voorbeeld Incident Management en responsebeleid • Handreiking Wijzigingsbeheer (in ontwikkeling) • Procedure Afvoer ICT middelen (in ontwikkeling) 	•						
Awareness informatiebeveiliging	• Presentatie borging awareness informatiebeveiliging incl. achtergrondinformatie	<ul style="list-style-type: none"> • Communicatieplan gemeente (in ontwikkeling) • Presentatie Bewustwording Informatieveiligheid bij gemeenten 	•	Ja, aanvullend op elkaar					
Meldplicht Datalekken en meldplicht Inbreuken op elektronische systemen	• Meldplicht Datalekken en meldplicht Inbreuken op elektronische systemen	•	•						
Responsible Disclosure	• Handreiking implementatie Responsible Disclosure	• Responsible Disclosure	• NCSC - Leidraad om te komen tot een praktijk van Responsible Disclosure	Ja, aanvullend op elkaar					
Authenticatie en Autorisatie (inclusief wachtwoorden)		<ul style="list-style-type: none"> • Toegangsbeleid • Wachtwoordbeleid • Telewerken beleid (in ontwikkeling) • Aanwijzing Logging 	•						

Onderwerp	CIP	BIG-OP	Overig	Bruikbaar Ja/Nee	Archetype				
					1	2	3	4	5
Inkopen / aanbesteding		<ul style="list-style-type: none"> Contractmanagement (in ontwikkeling) Inkoopvoorwaarden en informatiebeveiligingseisen Bewerkersovereenkomst Geheimhoudingsverklaring en BIG Handleiding screening personeel 							
Secure Software Development	Grip op Secure Software Development (zowel de eisen als proces)		<ul style="list-style-type: none"> NCSC – Paper 'ICT Beveiligingsrichtlijnen voor webapplicaties' CBP - Privacy by Design NIST: Special Publication SP800-53 'Recommended Security Controls for Federal Information Systems' ISO/IEC 27034-1 - Information technology -- Security techniques -- Application security (geen gratis document, part 1 published, rest in DRAFT) ISO/IEC 27034-2 - Organization normative framework (draft) ISO/IEC 27034-3 - Application security management process (pre-draft) ISO/IEC 27034-4 - Application security validation (pre-draft) ISO/IEC 27034-5 - Protocols and application security control data structure (draft) ISO/IEC 27034-6 - Security guidance for specific applications (draft) 	Input voor PvE voor het ontwikkelen van Software.					

Onderwerp	CIP	BIG-OP	Overig	Bruikbaar Ja/Nee	Archetype				
					1	2	3	4	5
Persoonsgegevens		<ul style="list-style-type: none"> Handreiking dataclassificatie Bewerkersovereenkomst 	<ul style="list-style-type: none"> CBP - Richtsnoeren beveiliging van persoonsgegevens CBP - Compliance-instrumenten 						
Medische gegevens		<ul style="list-style-type: none"> 	<ul style="list-style-type: none"> CBP - Medische gegevens 						
Testen met persoonsgegevens	Testen met persoonsgegevens buiten de productieomgeving	<ul style="list-style-type: none"> 	<ul style="list-style-type: none"> CBP - Handleiding Wet bescherming persoonsgegevens 						
Mobiele apparaten en telewerken		<ul style="list-style-type: none"> Telewerken beleid (in ontwikkeling) Mobiele gegevensdragers Mobile Device Management Hardening beleid voor gemeenten Anti-malware beleid 	<ul style="list-style-type: none"> 						
Cloudcomputing	Beveiligingsbeleid clouddiensten, v2.2 (excl. ADR)	<ul style="list-style-type: none"> Cloud Computing 	<ul style="list-style-type: none"> NCSC – Whitepaper 'Cloudcomputing & Security' 	Ja, aanvullend op elkaar					
Big Data		<ul style="list-style-type: none"> 	<ul style="list-style-type: none"> CBP- anonimiseer gegevens bij gebruik big data 						

Tabel 1 Informatiebeveiligingsonderwerpen

I